⑲日本国特許庁（JP）　⑪特許出願公開

⑫公開特許公報（A）　平1－307341

⑤Int.Cl.⁴		識別記号	庁内整理番号
H 04 L	11/26		7830－5K
H 04 B	7/26		M－7608－5K
H 04 L	9/02		Z－7240－5K
	11/00	310	B－7928－5K
	11/20	102	A－7830－5K

⑬公開　平成1年(1989)12月12日

審査請求　未請求　請求項の数 2　（全9頁）

⑭発明の名称　移動体データ暗号化通信方式

⑳特　願　昭63－137321
㉒出　願　昭63(1988)6月6日

⑫発明者　米元　英司　神奈川県川崎市中原区上小田中1015番地　富士通株式会社内
⑪出願人　富士通株式会社　神奈川県川崎市中原区上小田中1015番地
⑭代理人　弁理士　青木　朗　外4名

明　細　書

1. 発明の名称

移動体データ暗号化通信方式

2. 特許請求の範囲

1. 移動体通信装置（1）とパケット通信制御装置（2）とが無線接続され、パケット通信制御装置（2）と加入者装置（3）とが接続されて、パケット通信制御装置を介して移動体通信装置と加入者装置との間でデータ通信を行う通信方式において、

該移動体通信装置と該加入者装置とが、

通信路接続確立後、それぞれ原始鍵（α，β）に基いて生成した公開鍵（X，Y）を通信データとして送受し合い、

それぞれ受信した公開鍵に基いて共通のＤＥＳ暗号鍵（Z）を生成し、

該移動体通信装置と該加入者装置との間のデータ通信を、ＤＥＳ暗号鍵に基いて暗号化したデータを送信し、受信暗号化データをＤＥＳ暗号鍵を用いて復号するように構成したことを特徴とする、移動体データ暗号化通信方式。

2. 前記移動体通信装置と加入者装置との間の通信路接続確立、公開鍵送受信を無線チャネルの第1のチャネルを用いて行ない、

該第1のチャネルによる通信路を切断後、第2のチャネルにより通信路の接続確立を行ない、

第1のチャネルにより受信した公開鍵を用いて生成されたＤＥＳ暗号鍵を用いて、第2のチャネルにより、該移動体通信装置と該加入者装置との間の送受信データを暗号化、復号化するように構成したことを特徴とする、請求項1記載の移動体データ暗号化通信方式。

3. 発明の詳細な説明

〔概　要〕

テレターミナルシステム等の移動体通信方式に関し、

機密性が高く、処理の簡便な暗号化データ通信を行うことを目的にし、

移動体通信装置とパケット通信制御装置とが無線接続され、パケット通信制御装置と加入者装置

とが接続されて、パケット通信制御装置を介して移動体通信装置と加入者装置との間でデータ通信を行う無線通信方式において、該移動体通信装置と該加入者装置とが、通信路接続確立後、それぞれ原始鍵に基いて生成した公開鍵を通信データとして送受し合い、それぞれ受信した公開鍵に基いて共通のＤＥＳ暗号鍵を生成し、該移動体通信装置と該加入者装置との間のデータ通信を、ＤＥＳ暗号鍵に基いて暗号化したデータを送信し、受信暗号化データをＤＥＳ暗号鍵を用いて復号するように構成する。

〔産業上の利用分野〕

本発明は、移動体データ通信において機密性が高く処理が容易な通信方式に関する。

〔従来の技術〕

自動車電話、パーソナル無線などの移動体通信が発達につれて、企業内のホストコンピュータと、ルートセールス等の外勤員が携帯するデータ通信端末装置との間で、外勤員が出先で直接即時に、在庫照会、受発注業務を行う移動体データ通信の必要性が高まっている。すなわち、電話回線を用いて音響カップリングする方式ではなく、無線通信を行うものである。かゝる要望に対し、例えば、共同利用の無線ネットワークを用いて経済的で高品質な移動体データ通信路を提供するものとして、テレターミナルシステムの実用化が進められている。

第６図にテレターミナルシステムの構成図を示す。同図において、無線部、通信制御部およびデータ処理部を有する携帯端末１ａと無線部および通信制御部からなる無線基地局２ａとが無線接続されている。無線基地局は専用線によりパケット交換機２ｂに接続され、更にパケット交換機は専用線を介して加入者系のホストコンピュータ３ａに接続される。パケット交換機は、複数の無線基地局、複数の加入者系のホストコンピュータ等に接続される。

パケット交換機は共同利用センタに設置され、パケット交換機と無線基地局とで、共同利用ネットワーク設備を構成している。加入者系のホストコンピュータは、一般にＥＤＰ(Electrical Data Processing) を行なうように構成され、在庫管理、受発注処理等を行う。無線基地局は、大都市部においても、半径３km内にある携帯端末と無線接続されるように複数配置される。通信不能領域を生じさせないよう、無線基地局と無線接続される領域は、相互に重複する部分があるが、周波数が異ならせてある。これら重複する部分では、携帯端末は使用周波数を変えることで、２以上の無線基地局と無線接続が可能である。

以上の構成において、携帯端末は、無線基地局、パケット交換機を介して、所望のホストコンピュータと通信が可能となる。

第７図に、携帯端末から発呼を行って、ホストコンピュータとデータ通信を行う場合の通信手順（方法）を示す。携帯端末から発呼要求を出すと、パケット交換機で資格チェックを行ない、ホストコンピュータに接続要求を送出する。ホストコンピュータは通信路の接続を確認し、接続可能信号をパケット交換機に出力し、パケット交換機が無線基地局を介して発呼応答信号を携帯端末に送出する。携帯端末は発呼応答信号を受信することで、無線基地局およびパケット交換機を介した携帯端末とホストコンピュータとの通信路接続が確立される。次いで、必要な回数だけ、データ送信および返送データ送信が行なわれる。データ通信終了後、携帯端末から切断要求が出されると、パケット交換機において切断判定が行なわれ、携帯端末に切断応答が出力され、ホストコンピュータに切断指示が出力されることにより、通信路が切断される。

〔発明が解決しようとする課題〕

上述したテレターミナルシステムにおいては、携帯端末と無線基地局との間が無線接続されているので、この間のデータ通信は本来的に盗聴又は漏洩に対して無防備な状態にある。テレターミナルシステムを利用してルートセールスを行う場合

等、ホストコンピュータ内の在庫データ、携帯端末とホストコンピュータとの間の受発注データ等の企業にとって重要かつ機密性の高いデータが盗聴され易い環境におかれ、データの機密性に問題がある。また、誤ったデータが混入する場合も生ずる。

以上、テレターミナルシステムを例示したが、他の移動体データ通信方式においても上記同様の問題が生ずる。

データ通信の機密性を向上させる手段の1つに、暗号化通信があるが、テレターミナルシステムを始めとする移動体データ通信方式においては、暗号化通信は殆んど適用されていない。その理由の1つとしては、機密性の高い暗号化通信を行うには、相当複雑な回路が必要となるが、携帯端末などの移動体側にかゝる回路を設けることは、価格、寸法的に難しいことがある。また、特にテレターミナルシステムのように、多数の携帯端末と多数のホストコンピュータとの間でデータ通信を行う場合、それぞれの携帯端末とホストコンピュータで複雑な暗号化を行うことは特に難しい。

暗号化技術としては、大規模なホストコンピュータ相互間で行なわれている「公開鍵方式」等と、比較的簡単な装置相互間で用いられる「ＤＥＳ(Data Encryption Standard)方式」等が知られている。公開鍵方式はデータ通信毎、配送された公開鍵から暗号鍵を生成し、この暗号鍵に基いて暗号化データ通信を行う。一方ＤＥＳ方式は、暗号強度が強く、且つ比較的簡単な回路で暗号化、復号化の処理が行える方式で固定鍵を用いて暗号化データ通信を行う。

これらの暗号化方式をテレターミナルシステム等の移動体データ通信に用いると次のような問題が生じる。先ず、公開鍵方式は、暗号鍵の生成および復号のために相当時間がかゝり、携帯端末の如き小形の装置では、データ通信毎暗号鍵の生成、復号を行うことが実質的にできない。一方、ＤＥＳ方式は、固定鍵を用いているため長時間同じ固定鍵を用いていると盗聴により解読される可能性が生じる。そこで、固定鍵をひんぱんに代える必要があるが、1台のホストコンピュータに対し多数の携帯端末が接続されるテレターミナルシステム等において、同時に、ホストコンピュータと多数の携帯端末の固定鍵を代えることは実質的に不可能であるし、その作業が大変であり、また複雑な管理が必要になる。従って、従来の暗号技術をそのまゝ適用することはできない。

以上に述べたように、本発明は、テレターミナルシステム等の移動体データ通信方式において、機密性が高くしかも処理が簡便な暗号化データ通信を可能にすることを目的とする。

〔課題を解決するための手段、および、作用〕

第2図に本発明が適用される移動体データ暗号化通信方式の構成図を示す。同図において、1は、第6図のテレターミナルシステムの携帯端末等に対応する移動体通信装置、2は第6図の無線基地局およびパケット交換機に相当するパケット通信制御装置、3は第6図のホストコンピュータに対応する加入者装置を示す。移動体通信装置1とパケット通信制御装置2とは無線接続される。

第1図（ａ）に、移動体通信装置1および加入者装置3のそれぞれに組込まれる本発明の移動体データ暗号化通信方式の通信処理方法の原理ブロック図を示す。

該移動体通信装置と該加入者装置とが、通信路接続確立後、それぞれ原始鍵α，βに基いて生成した公開鍵Ｘ，Ｙを送受し合う。次いで、それぞれ受信した公開鍵に基いて共通のＤＥＳ暗号鍵Ｚを生成する。その後、該移動体通信装置と該加入者装置との間のデータ通信を、ＤＥＳ暗号鍵に基いて暗号化したデータを送信し、受信暗号化データをＤＥＳ暗号鍵を用いて復号する。

すなわち、機密性が高い一方演算時間のかゝる公開鍵の生成は、通信の初めの段階で一度だけ行ない、各データ通信における暗号化又は復号化は公開鍵に基いて生成した演算の簡単なＤＥＳ暗号鍵に基いて行う。これにより、機密性を高く維持しつつ、簡易且つ高速な暗号化データ通信が可能になる。

本発明の第2の形態として、移動体通信装置1および加入者装置3のそれぞれに組込れる通信方法の原理ブロック図を第1図（b）に示す。

第1図（b）において、まず、前記移動体通信装置と加入者装置との間の通信路接続確立、公開鍵送受信を無線チャネルの第1のチャネルを用いて行ない、一旦、該第1のチャネルによる通信路を切断する。次いで、第2のチャネルにより通信路の接続確立を行ない、第1のチャネルにより受信した公開鍵を用いて生成されたＤＥＳ暗号鍵を用いて、第2のチャネルにより、該移動体通信装置と該加入者装置との間の送受信データを暗号化、復号化する。

かゝる構成によれば、ＤＥＳ暗号鍵の生成に用いるチャネルと暗号化データ通信に用いるチャネルとは異なるから、たとえ公開鍵が盗聴されてＤＥＳ暗号鍵が解読されるような事態が発生しても、更に、異なるチャネルによる暗号化データの解読は困難である。

〔実施例〕

本発明の実施例として第6図のテレターミナルシステムの場合を例示して述べる。

第3図（a）（b）にそれぞれ、第6図のテレメータシステムにおける発呼要求パケットおよびデータ送信パケットのデータフォーマット図を示す。

第4図を参照して本発明の第1実施例について述べる。第4図は、携帯端末1aから発呼要求が出力される場合の、携帯端末1a、無線基地局2aおよびパケット交換機2b、ホストコンピュータ3aとの間の通信方法を示す。従って、携帯端末1a、無線基地局2a、パケット交換機2bおよびホストコンピュータ3aは、第4図を参照して述べる下記の動作が可能な回路に構成されている。

第4図は、大別すると、通信路接続確立、暗号鍵生成、暗号化データ通信、および通信路切断の処理方法を示している。但し、これらの通信は1つのチャネル（1つの無線周波数帯）を用いて行う。

A．通信路接続確立

携帯端末1aから第3図（a）のデータフォーマットに従って、自己の端末ＩＤ（識別）コードを送信装置ＩＤ、送信先のホストコンピュータのＩＤコードを受信装置ＩＤとして、発呼要求を行う。無線基地局2aは発呼要求を受信し、その受信データについてパケット交換機2bが、資格チェックを行う。すなわち、送信元と受信先とが正常であることをチェックする。資格チェックが正しい場合、パケット交換機2bから対応するホストコンピュータ3aに「接続要求」が送出される。

ホストコンピュータ3aは「接続要求」を受信し、接続可能な場合「接続確認」を返送する。この返送信号は、パケット交換機2b、無線基地局2aを介して携帯端末1aに接続可能であることを示す「発呼応答」として送信される。

以上により、通信路の接続が確立される。

尚、無線ネットワーク上では、第3図（a）（b）に図示の如く、無線プロトロルに準拠した、ガードビッド（ＧＢ）、ビット同期信号（ＢＳ）、フレーム同期信号（ＦＳ）、ＣＲＣチェック符号、誤り訂正パリティがつけられたパケットデータとして通信される。テレターミナルシステムにおいては、無線区間は、無線基地局からの制御チャネルの信号（Ｃ）により使用可能通信チャネルの指定がされており、各端末は自由に通信チャネルを選んで発呼できる。また各チャネルはパケット毎のスロットに区切られ、携帯端末はこのスロットを使ってデータ通信を行う。

B．暗号鍵生成

携帯端末1a、ホストコンピュータ3aはそれぞれ予め、ランダムに創った原始鍵α，βから次の演算を行い、それぞれ公開鍵Ｘ，Ｙを生成する。

$$X = M^{\alpha} \cdots (1)$$

$$Y = M^{\beta} \cdots (2)$$

次いで、生成された公開鍵Ｘ，Ｙを相互に送受信して、交換し合う。この場合、公開鍵Ｘ，Ｙはそれぞれ、第3図（b）のデータ送信パケットの利用者データ部にセットされて送信される。

更に、携帯端末1a、ホストコンピュータ3a

は、それぞれ、自己の原始鍵α，βと受信した公開鍵X，Yにもとづいて、DES暗号鍵Z₁，Z₂を生成する。

$$Z_1 = Y^{\alpha} = M^{\alpha\beta} \quad \cdots (3)$$

$$Z_2 = X^{\beta} = M^{\alpha\beta} \quad \cdots (4)$$

式（3），（4）から明らかなように、$Z_1 = Z_2$、すなわち、DES暗号鍵Z₁，Z₂は等しい。従って、携帯端末1aにおいてDES暗号鍵Z₁を用いて暗号化したデータをホストコンピュータ3aに送信した場合、ホストコンピュータ3aは受信データをDES暗号鍵Z₂を用いて復号（解読）することができる。ホストコンピュータ3aから携帯端末1aに暗号化データを送信する場合も同様である。このようにDES暗号鍵Z₁，Z₂は共通のDES暗号鍵$Z = Z_1 = Z_2$となっている。

C．暗号化データ通信

以上の如く、共通のDES暗号鍵Zが生成されたら、携帯端末1aは、この暗号鍵Z₁を用いて送信データを暗号化し、暗号化データを送信する。暗号化データは、第3図（b）の利用者データ部にセットされる。一方、ホストコンピュータ3aは暗号鍵Z₂を用いて受信暗号化データを復号し、返送データを暗号鍵Z₂を用いて暗号化する。この場合の暗号化データも第3図（b）の利用者データ部にセットされる。携帯端末1aは受信返送暗号化データを暗号鍵Z₁を用いて復号する。

パケット交換において利用者データ部は16バイトであるから、送信データ長に応じて、以上の暗号化データ通信をくり返す。

D．通信路切断

所望の暗号化データ通信が終了すると、携帯端末1aから切断要求が出力され、第7図を参照して述べた従来方法と同様の処理により、通信路が切断される。

上記実施例において、公開鍵X，Y自体は盗聴される可能性があるが、公開鍵X，Yが盗聴されたとしても、原始鍵α，βの機密が保たれている限り、これらX，Yから共通のDES暗号鍵Zを逆算するには、超大形コンピュータを用いても、ぼう大な演算時間がかゝるので、暗号化データが第三者によって解読されることは事実上ない。すなわち、原始鍵を用いて公開鍵を生成し、更に相互に交換した公開鍵と原始鍵を用いて共通のDES暗号鍵を生成し、このDES暗号鍵を用いて暗号化データ通信を行えば、非常に機密性の高い暗号化データ通信が可能となる。更に機密性を向上させるために、原始鍵α，βは通信路接続を開始する毎に、ランダムに異なった値が選ばれており、公開鍵X，Yも毎回新しい値となっている。

また、比較的演算量が多く演算時間のかゝる公開鍵の生成およびDES暗号鍵の生成は暗号化データ通信の度に行うのではなく、通信の初期段階に行ない、しかも簡便なDES暗号鍵を用いて暗号化データ通信を行うので、暗号化データ通信によってもそれ程通信時間が長くなることもない。更に、公開鍵の生成、DES暗号鍵の生成を初期段階にのみ行うので、多少演算時間がかゝってもよく、特に、携帯端末に高速演算回路を設ける必要はなく、携帯端末を大規模化、高価格する必要はない。

暗号化データ通信によっても、無線基地局、パケット交換機にとって利用者データ部のデータは暗号化の有無に拘らず、単なるデータに過ぎないからこれら無線基地局、パケット交換機は、何ら変更は必要ない。

以上の暗号化データは、携帯端末1aと無線基地局2aとの間の無線部における盗用に対して機密性を有するばかりでなく、無線基地局～ホストコンピュータの間の通信路における盗用に対しても機密性を有する。

第5図を参照して本発明の第2実施例を述べる。

第2実施例は、更に機密性を向上させるものである。このため、公開鍵交換に係る通信のチャネルと、DES暗号化通信に用いるチャネルとを異ならせている。パケット交換においては、携帯端末およびホストコンピュータは複数のチャネルを使用できるから、このようにチャネルを異ならせて使用できる。通信路接続確立、公開鍵生成、公開鍵交換、DES暗号鍵生成、通信路切断、DE

S暗号化データ通信のそれぞれの処理は第1実施例と同様である。

第2実施例においては、万一、公開鍵が盗聴されてDES暗号鍵が解読されたとしても、DES暗号化データ通信は携帯端末が任意に選べる別のチャネルで行なわれているので、暗号データが解読されることはない。このため、公開鍵の生成、交換、DES暗号鍵の生成を、通信の度に行う必要はなく、例えば、10回に1度の如く低下させ、暗号鍵生成・通信時間を少なくすることができる。

以上の実施例は、テレターミナルシステムを例示して述べたが、本発明は、パーソナル無線その他の移動体データ暗号化通信システムにも適用できる。

〔発明の効果〕

以上に述べたように本発明によれば、原始鍵を用いて公開鍵を生成し更に交換し合った公開鍵とそれぞれの原始鍵によって共通のDES暗号鍵を生成し、この機密性の高いDES暗号鍵を用いてデータの暗号化、復号化を行うので、無線区間を介してデータ通信を行っても、データの機密性を非常に高く維持することができるという効果を奏する。

更に本発明によれば、暗号鍵生成時のチャネルと暗号化データ通信時のチャネルとを異ならせることにより、データの機密性がさらにもう一段高くなるという効果を奏する。

4. 図面の簡単な説明

第1図(a)(b)は本発明の移動体データ暗号化通信方式の通信処理方法の原理ブロック図、

第2図は本発明の移動体データ暗号化通信方式の構成図、

第3図(a)(b)は本発明の実施例のパケットデータフォーマット図、

第4図および第5図は本発明の第1および第2の実施例の暗号化通信方法を示す図、

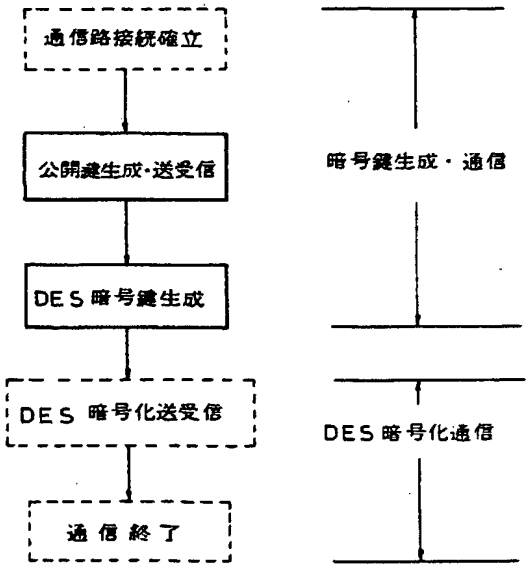
第6図はテレターミナルシステム構成図、

第7図は従来のテレターミナルシステムにおけるデータ通信方法を示す図、である。

(符号の説明)

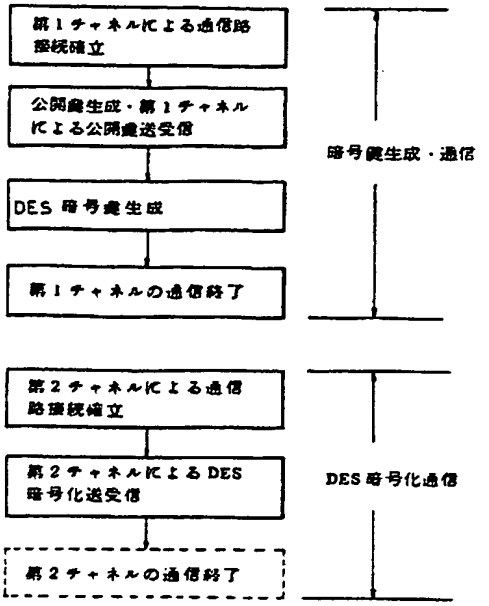
1…移動体通信装置、
2…パケット通信制御装置、
3…加入者装置、　1a…携帯端末、
2a…無線基地局、　2b…パケット交換機、
3a…ホストコンピュータ。

特許出願人
富士通株式会社
特許出願代理人
弁理士　青木　朗
弁理士　石田　敬
弁理士　平岩賢三
弁理士　山口昭之
弁理士　西山雅也



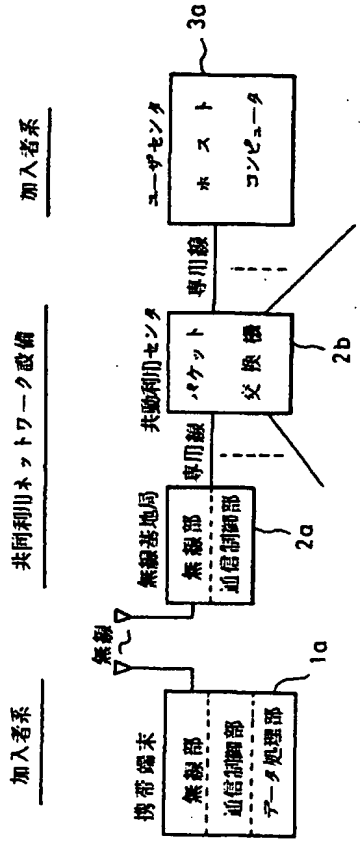
本発明の移動体データ暗号化通信方式の通信処理方法の原理ブロック図

第1図(a)



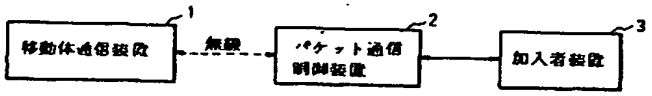
本発明の移動体データ暗号化通信方式の通信処理方法の原理ブロック図

第 1 図(b)



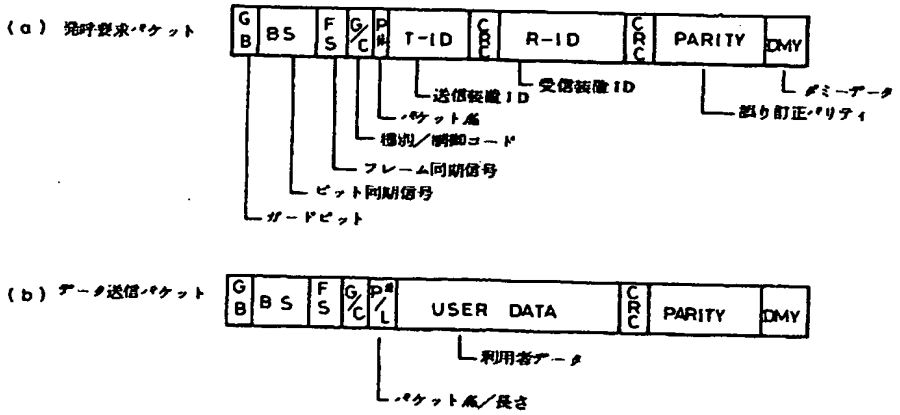
テレターミナルシステム構成図

第 6 図



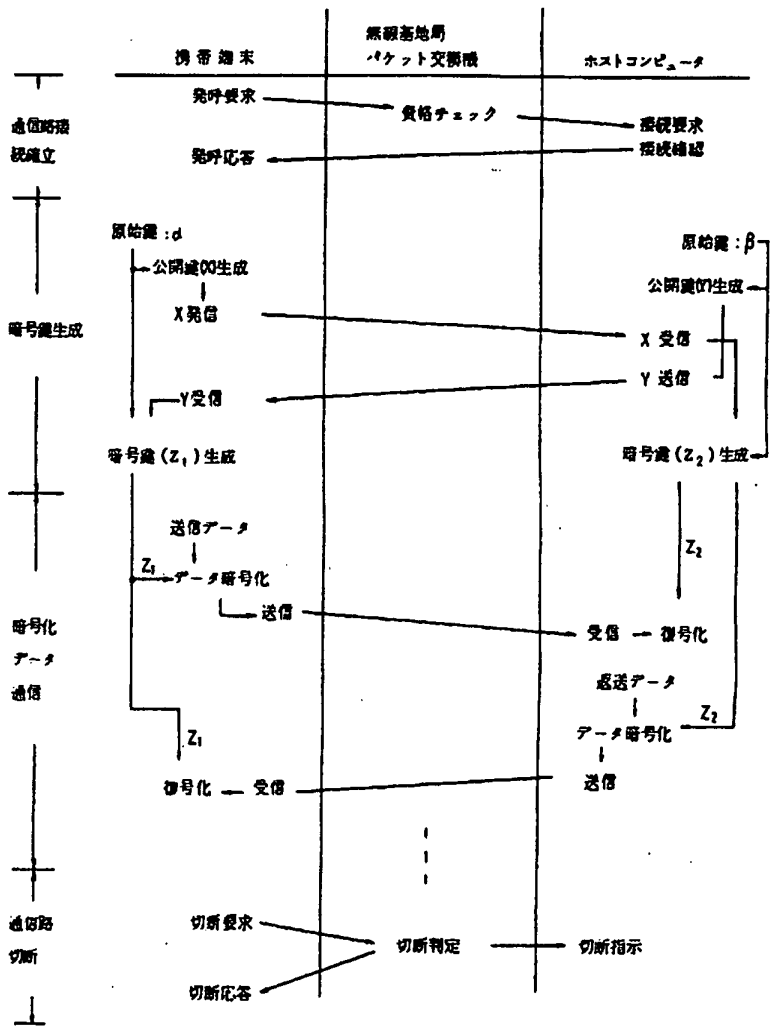
本発明の移動体データ暗号化通信方式の構成図

第 2 図



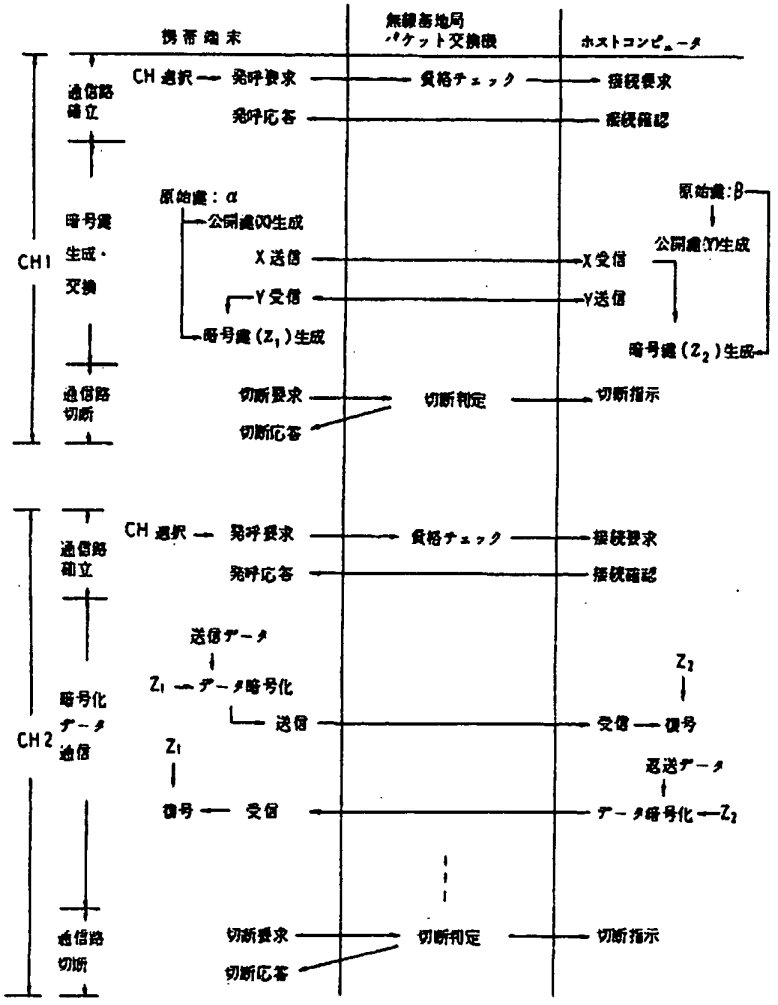
本発明の実施例のパケットデータフォーマット図

第 3 図



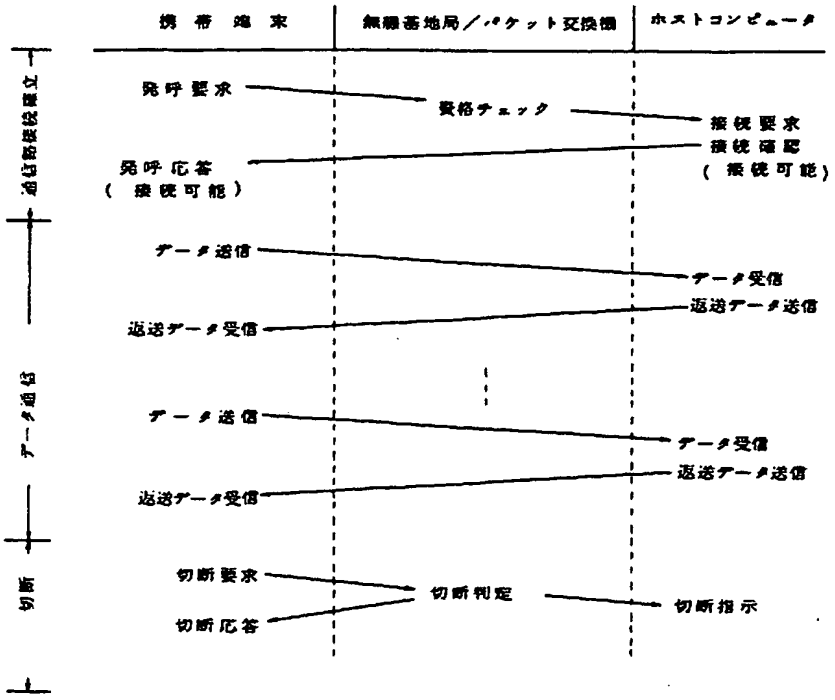
本発明の第2実施例の暗号化通信方法を示す図

第5図



本発明の第1実施例の暗号化通信方法を示す図

第4図



第6図テレターミナルシステムにおける従来のデータ通信方法を示す図

第 7 図